UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

In Re: Overby-Seawell Company Customer Data Security Breach Litigation	Case No. 1:23-md-03056-SDG
	CLASS ACTION
This Document Relates to: Case No. 1:22-cv-03708-SDG	JURY TRIAL DEMANDED

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiff Kathy Keefer ("Plaintiff"), individually, and on behalf of all others similarly situated (collectively, "Class members"), by and through her attorneys, brings this First Amended Class Action Complaint against Overby-Seawell Company ("OSC") and Fulton Bank, N.A. ("Fulton") (collectively, "Defendants") and complains and alleges upon personal knowledge as to herself and information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to secure and safeguard her and at least 111,663 other individuals' personally identifiable information ("PII"), including names, loan numbers, mailing addresses,

collateral addresses, telephone numbers, loan amounts, loan maturity dates, insurance policy information, and Social Security numbers.

2. OSC is a company that provides various services to financial companies, such as compliance, tracking, outsourcing, and insurance services.

3. Fulton is a bank that operates in Pennsylvania, New Jersey, Delaware, Maryland, and Virginia. Fulton provides PII to OSC in connection with receiving property insurance validation.

4. Between May 26, 2022 and July 5, 2022, unauthorized individuals had access to OSC's network systems and acquired the PII of Plaintiff and Class members (the "Data Breach").

5. Defendants owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII against unauthorized access and disclosure. Defendants breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect their PII from unauthorized access and disclosure.

6. As a result of Defendants' inadequate security and breach of their duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII was accessed and disclosed. This action seeks to remedy these failings and their

consequences. Plaintiff brings this action on behalf of herself and all persons whose PII was exposed as a result of the Data Breach, which OSC learned of on or about July 5, 2022.

7. Plaintiff, on behalf of herself and all other Class members, asserts claims for negligence, negligence per se, breach of implied contract, unjust enrichment, and violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Law, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

8. Plaintiff Kathy Keefer is a Pennsylvania resident. She received a letter from OSC notifying her that her PII was accessed in the Data Breach. Plaintiff Keefer would not have sought a loan from or provided her PII to Fulton had she known that Defendants would not adequately protect her PII.

9. Defendant Overby-Seawell Company is a Georgia corporation. OSC's principal place of business is located at 245 TownPark Drive, Ravine One, Suite 200, Kennesaw, GA 30144.

10. Defendant Fulton Bank, N.A. is a Pennsylvania corporation. Fulton's principal place of business is located at 1 Penn Square, Lancaster, PA 17602.

JURISDICTION AND VENUE

11. The Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

12. This Court has personal jurisdiction over OSC because OSC has its principal place of business in Georgia.

13. The Court has personal jurisdiction over Fulton because Fulton contracted with OSC, which is a Georgia corporation, and shared Plaintiff's PII with OSC in Georgia.

14. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because OSC's principal place of business is located in Cobb County, Georgia, Fulton provided OSC with the PII of Plaintiff in this District, and a substantial part of the events giving rise to Plaintiff's claims arose in this District.

FACTUAL ALLEGATIONS

Overview of Defendants

15. OSC claims to be "a leading provider of compliance-driven tracking technology and insurance products and services for lenders, mortgage servicers and

property investors."[1] The company states that it "deliver[s] competitive insurance solutions . . . from a variety of top-rated carriers who specialize in this space."[2]

16. Fulton "offers a broad array of financial products and services in Pennsylvania, New Jersey, Maryland, Delaware, and Virginia."[3] The company has "over 200 financial centers and specialty offices and over 230 ATMs."[4]

17. In the regular course of their business, Defendants collect and maintain the PII of their clients and their clients' customers.

18. OSC's website contains a privacy policy which states, "The privacy of personal client information is important to Breckenridge IS, LLC, and its subsidiaries and affiliates (collectively "Breckenridge IS" including the Overby-Seawell Co. called "OSC")."[5] It goes on to state, "At Breckenridge IS and OSC, we strive always to maintain the highest level of confidentiality for our Participants."[6]

---

[1] *Who We Are*, OSC, https://www.oscis.com/who-we-are/ (last accessed Mar. 10, 2023).
[2] *Insurance*, OSC, https://www.oscis.com/insurance/ (last accessed Mar. 10, 2023).
[3] *About Fulton Bank*, FULTON BANK, https://www.fultonbank.com/About-Fulton-Bank (last accessed Mar. 10, 2023).
[4] *Id*.
[5] *Privacy Policy*, OSC, https://www.oscis.com/privacy/ (last accessed Mar. 10, 2023).
[6] *Id*.

19. The privacy policy that Fulton Bank has on its website starts, "Your privacy is very important to us."[7] It also states, "We take our responsibility to protect your Personal Information very seriously. To protect Personal Information from unauthorized access and use, we apply administrative, technical and physical security measures that comply with applicable federal and state laws."[8]

20. Plaintiff and Class members are, or were, customers of OSC's clients, including Fulton, and entrusted OSC with their PII through OSC's clients.

The Data Breach

21. Between May 26, 2022 and July 5, 2022, an unauthorized individual, or unauthorized individuals, had access to OSC's network systems and took files from OSC's network systems."[9] The information included PII for customers of Fulton Bank.[10]

22. OSC did not begin to notify government agencies or the public about the Data Breach until almost two months after the discovery of the breach, on or

---

[7] *Fulton Financial Corporation Consumer Privacy Policy*, FULTON BANK, https://www.fultonbank.com/Security/Consumer-Privacy-Notice (last accessed Mar. 10, 2023).
[8] *Id*.
[9] *Fulton Bank Data Breach Notice to Consumers*, OFFICE OF THE VERMONT ATTORNEY GENERAL, https://www.mass.gov/doc/assigned-data-breach-number-28164-fulton-financial-corporation/download (last accessed Mar. 10, 2023).
[10] *Id*.

about August 30, 2022. Thus, Plaintiff's and Class members' PII was in the hands of cybercriminals for almost two months before they were warned that the Data Breach may have affected this information.

23. The notice that OSC sent to those affected by the breach states the information that was disclosed included a persons' "name, loan number, mailing address, collateral address, telephone number, loan amount, loan maturity date, and insurance policy information."[11] The letter also states, "Your social security number was also contained in those files."[12]

24. The information of at least one other client of OSC was also involved in the Data Breach.[13] It is currently unclear how many other persons' PII was involved in the Data Breach.

Defendants Knew that Criminals Target PII

25. At all relevant times, Defendants knew, or should have known, that the PII that they collected was a target for malicious actors. Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate data

[11] *Id*.
[12] *Id*.
[13] Frank Bajak, *KeyBank: Hackers of Third-Party Provider Stole Customer Data*, AP NEWS (Sep. 3, 2022), https://apnews.com/article/technology-hacking-data-privacy-23b0d233ddaf6fee4831f69e7b113848.

privacy and security measures to protect Plaintiff's and Class members' PII from cyber-attacks that Defendants should have anticipated and guarded against.

26. It is well known among companies that store sensitive personally identifying information that sensitive information—such as the Social Security numbers ("SSNs") and financial information stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[14]

27. PII is a valuable property right.[15] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[16] American companies are estimated to have spent over $19 billion on

[14] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019, 8:05 A.M.), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

[15] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

[16] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD iLIBRARY (April 2, 2013),

acquiring personal data of consumers in 2018.[17] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

28. As a result of their real and significant value, identity thieves and other cyber criminals have openly posted credit card numbers, SSNs, PII, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated and become more valuable to thieves and more damaging to victims.

29. Consumers place a high value on the privacy of that data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[18]

---

https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[17] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[18] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

30. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII Has Grave and Lasting Consequences for Victims

31. Theft of PII is serious. The FTC warns consumers that identity thieves use PII to receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[19]

32. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[20] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and

[19] *See* Federal Trade Commission, *What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Mar. 10, 2023).

[20] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[21]

33. With access to an individual's PII, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: opening utility accounts using the victim's identity; file a fraudulent tax return using the victim's information; or even give the victim's personal information to police during an arrest.[22]

34. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need

[21] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN, https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/ (last accessed Mar. 10, 2023).

[22] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Mar. 10, 2023).

more than a month to resolve issues stemming from identity theft and some need over a year.[23]

35. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

36. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (*e.g.*, name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[24]

37. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used.

---

[23] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last accessed Mar. 10, 2023).

[24] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[25]

38. It is within this context that Plaintiff and Class members must now live with the knowledge that their PII is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

Damages Sustained by Plaintiff and the Other Class Members

39. Plaintiff and Class members have suffered injury and damages, including, but not limited to: (i) a substantially increased risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

[25] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

CLASS ACTION ALLEGATIONS

40. This action is brought and may be properly maintained as a class action pursuant to Federal Rule of Civil Procedure 23.

41. Plaintiff brings this action on behalf of herself and all members of the following Class of similarly situated persons:

> All persons whose PII was accessed by unauthorized persons in the Data Breach, including all who were sent a notice of the Data Breach (the "Nationwide Class")

42. Plaintiff alternatively brings this action on behalf of herself and all members of the following subclass of similarly situated persons:

> All persons who provided their PII to Fulton Bank, N.A. and whose PII was disclosed to unauthorized persons in the Data Breach, including all persons who provided their PII to Fulton Bank, N.A. and were sent a notice of the Data Breach (the "Fulton Subclass").[26]

43. Excluded from the Class is Overby-Seawell Company and Fulton Bank, N.A. and their affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

44. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the

[26] The Nationwide Class and the Fulton Subclass are collectively referred to as the "Class."

same evidence as would be used to prove those elements in individual actions alleging the same claims.

45. The members of the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. OSC reported to the Maine Attorney General that approximately 111,663 persons' information was exposed in the Data Breach.[27]

46. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether Defendants had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class members' PII from unauthorized access and disclosure;

b. Whether Defendants failed to exercise reasonable care to secure and safeguard Plaintiff's and Class members' PII;

c. Whether an implied contract existed between Class members and Defendants, providing that Defendants would implement and

[27] *Data Breach Notifications*, Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/ed302996-9b56-4ec2-af8f-5d9ee7ee8fef.shtml (last accessed Mar. 10, 2023).

maintain reasonable security measures to protect and secure Class members' PII from unauthorized access and disclosure;

d. Whether Defendants breached their duties to protect Plaintiff's and Class members' PII; and

e. Whether Plaintiff and Class members are entitled to damages and the measure of such damages and relief.

47. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

48. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had her PII compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendants, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

49. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that she has no interests adverse to, or that conflict with, the Class she seeks to represent. Plaintiff

has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

50. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for Class members to individually seek redress from Defendants' wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

51. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

52. Plaintiff brings this claim against Overby-Seawell Company on behalf of both the Nationwide Class and the Fulton Subclass and brings this claim against Fulton Bank, N.A. on behalf of the Fulton Subclass.

53. Defendants owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting their PII in their possession, custody, or control.

54. Defendants knew the risks of collecting and storing Plaintiff's and Class members' PII and the importance of maintaining secure systems. Defendants knew of the many data breaches that targeted companies that stored PII in recent years.

55. Given the nature of Defendants' business, the sensitivity and value of the PII it maintains, and the resources at their disposal, Defendants should have identified the vulnerabilities to their systems and prevented the Data Breach from occurring.

56. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and

software and hardware systems to safeguard and protect PII entrusted to it—including Plaintiff's and Class members' PII.

57. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII to unauthorized individuals.

58. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII would not have been compromised.

59. As a result of Defendants' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation

of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

COUNT II
NEGLIGENCE PER SE

60. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

61. Plaintiff brings this claim against Overby-Seawell Company on behalf of both the Nationwide Class and the Fulton Subclass and brings this claim against Fulton Bank, N.A. on behalf of the Fulton Subclass.

62. Defendants' duties arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as Defendants, of failing to employ reasonable measures to protect and secure PII.

63. Defendants violated Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and Class members' PII and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtains and stores, and the foreseeable

consequences of a data breach involving PII including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

64. Defendants' violation of Section 5 of the FTCA constitutes negligence per se.

65. Defendants and Class members are within the class of persons that Section 5 of the FTCA was intended to protect.

66. The harm occurring as a result of the Data Breach is the type of harm Section 5 of the FTCA weas intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair practices or deceptive practices, caused the same type of harm that has been suffered by Plaintiff and Class members as a result of the Data Brach.

67. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII to unauthorized individuals.

68. The injury and harm that Plaintiff and Class members suffered was the direct and proximate result of Defendants' violations of Section 5 of the FTCA. Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

COUNT III
BREACH OF IMPLIED CONTRACT

69. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

70. Plaintiff brings this claim against Overby-Seawell Company on behalf of both the Nationwide Class and the Fulton Subclass and brings this claim against Fulton Bank, N.A. on behalf of the Fulton Subclass.

71. In connection with the dealings Plaintiff and Class Members had with Defendants, Plaintiff and Class members entered into implied contracts with Defendants.

72. Pursuant to these implied contracts, Plaintiff and Class members provided Defendants with their PII, directly or indirectly, in order for Defendants to provide services. In exchange, Defendants agreed to, among other things, and Plaintiff and Class members understood that Defendants would: (1) provide services to Plaintiff and Class member; (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII; and (3) protect Plaintiff's and Class members PII in compliance with federal and state laws and regulations and industry standards.

73. The protection of PII was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and Defendants, on the other hand. Indeed, Defendants were clear in their privacy policies, and Plaintiff understood, that Defendants supposedly respect and are committed to protecting customer privacy.

74. Had Plaintiff and Class members known that Defendants would not adequately protect their customers' and former customers' PII, they would not have provided Defendants with their PII.

75. Plaintiff and Class members performed their obligations under the implied contracts when they provided Defendants with their PII, either directly or indirectly.

76. Defendants breached their obligations under their implied contracts with Plaintiff and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class members' PII in a manner that complies with applicable laws, regulations, and industry standards.

77. Defendants' breach of their obligations of the implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the injuries that Plaintiff and all other Class members have suffered from the Data Breach.

78. Plaintiff and all other Class members were damaged by Defendants' breach of implied contracts because: (i) they paid—directly or indirectly—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII has been breached; (v) they were deprived of the value of their PII, for which there is a well-

established national and international market; and (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face.

COUNT IV
UNJUST ENRICHMENT

79. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

80. This claim is pleaded in the alternative to the breach of implied contract claim.

81. Plaintiff brings this claim against Overby-Seawell Company on behalf of both the Nationwide Class and the Fulton Subclass and brings this claim against Fulton Bank, N.A. on behalf of the Fulton Subclass.

82. Plaintiff and Class members conferred a monetary benefit upon Defendants in the form of monies paid for services to Fulton, which Fulton used to acquire services from OSC.

83. Defendants accepted or had knowledge of the benefits conferred upon them by Plaintiff and Class members. Defendants also benefitted from the receipt of Plaintiff's and Class members' PII, as this was used in providing the printing or other services.

84. As a result of Defendants' conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

85. Defendants should not be permitted to retain the money belonging to Plaintiff and Class members because Defendants failed to adequately implement the data privacy and security procedures for themselves that Plaintiff and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

86. Defendants should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT V
VIOLATIONS OF THE PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW ("UTPCPL") 73 P.S. §§ 201-1–201-9.3

87. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

88. Plaintiff brings this claim against Overby-Seawell Company on behalf of both the Nationwide Class and the Fulton Subclass and brings this claim against Fulton Bank, N.A. on behalf of the Fulton Subclass.

89. Defendants both perform services in the Commonwealth of Pennsylvania or market services in the Commonwealth of Pennsylvania.

90. Plaintiff, Class members, and Defendants are "persons" as defined by the UTPCPL. 73 P.S. § 201-2(2).

91. Fulton's financial services and OSC's services performed for Fulton constitute as "trade" and "commerce" under the statute. 73 P.S. § 201-2(3).

92. Defendants obtained Plaintiff's and Class members' PII in connection with Fulton's financial services and OSC's services performed on behalf of Fulton.

93. Defendants engaged in unfair or deceptive acts in violation of the UTPCPL by failing to implement and maintain reasonable security measures to protect and secure their customers' PII in a manner that complied with applicable laws, regulations, and industry standards.

94. Defendants make explicit statements to their customers that their PII will remain private, as evidenced by their privacy policies.

95. The UTPCPL lists twenty-one instances of "unfair methods of competition" and "unfair or deceptive acts or practices." 73 P.S. § 201-2(4). Defendants' failure to adequately protect Plaintiff and Class members' PII while holding out that they would adequately protect the PII falls under at least the following categories:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation or connection that he does not have (73 P.S. § 201-2(4)(v));

b. Representing that goods or services are of a particular standard, quality or grade, or that goods are of a particular style or model, if they are of another (73 P.S. § 201-2(4)(vii));

c. Advertising goods or services with intent not to sell them as advertised (73 P.S. § 201-2(4)(ix)); and

d. Engaging in any other fraudulent or deceptive conduct which creates a likelihood of confusion or of misunderstanding (73 P.S. § 201-2(4)(xxi)).

96. Due to the Data Breach, Plaintiff and Class members have lost property in the form of their PII. Further, Defendants' failure to adopt reasonable practices in protecting and safeguarding their customers' PII will force Plaintiff and Class members to spend time or money to protect against identity theft. Plaintiff and Class members are now at a higher risk of identity theft and other crimes. This harm sufficiently outweighs any justifications or motives for Defendants' practice of collecting and storing PII without appropriate and reasonable safeguards to protect such information.

97. As a result of Defendants' violations of the UTPCPL, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

98. Pursuant to 73 P.S. § 201-9.2(a), Plaintiff seeks actual damages, $100, or three times their actual damages, whichever is greatest. Plaintiff also seeks costs and reasonable attorney fees.

PRAYER FOR RELIEF

Plaintiff, individually, and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in her favor and against Defendants as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of herself and the Class, seeks appropriate injunctive relief designed to prevent Defendants from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend credit monitoring services and similar services to protect against all types of identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this First Amended Class Action Complaint so triable.

Dated: May 1, 2023

Respectfully submitted,

/s/ Ben Barnow

Ben Barnow*
Anthony L. Parkhill*
Riley W. Prince*
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Tel: 312.621.2000
Fax: 312.641.5504
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com
rprince@barnowlaw.com

James M. Evangelista (GA Bar No. 707807)

EVANGELISTA WORLEY, LLC
500 Sugar Mill Road, Ste. 245A
Atlanta, GA 30350
(404) 205-8400
jim@ewlawllc.com

Counsel for Plaintiff Kathy Keefer
*admitted pro hac vice